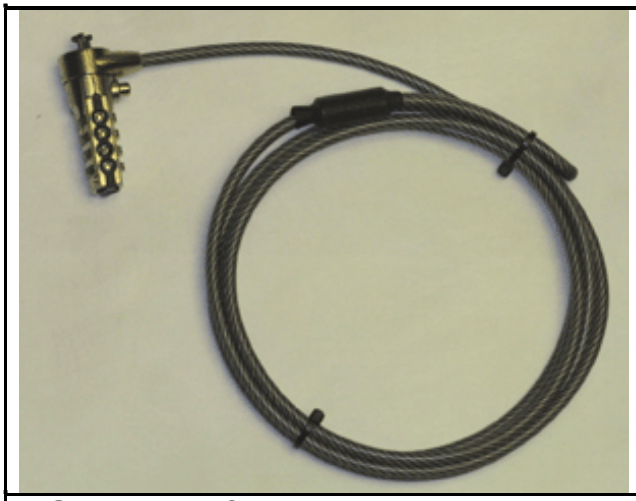
TARGUS DEFCON CL® MODEL PA410U and ASP10US

Marc Weber Tobias and Matthew Fiddler

September 11, 2006

	
MODEL PA410U	**MODEL ASP10US**

A simple method of covert bypass renders the new Targus DEFCON CL lock vulnerable to compromise in seconds. The same locking mechanism is utilized in the two models shown above. Two techniques of forced entry are also disclosed that allow the cable to be cut rapidly. This report details security vulnerabilities regarding both the standard and armored versions of this lock. In our opinion, this lock is not secure and should not be relied upon for any real measure of security.

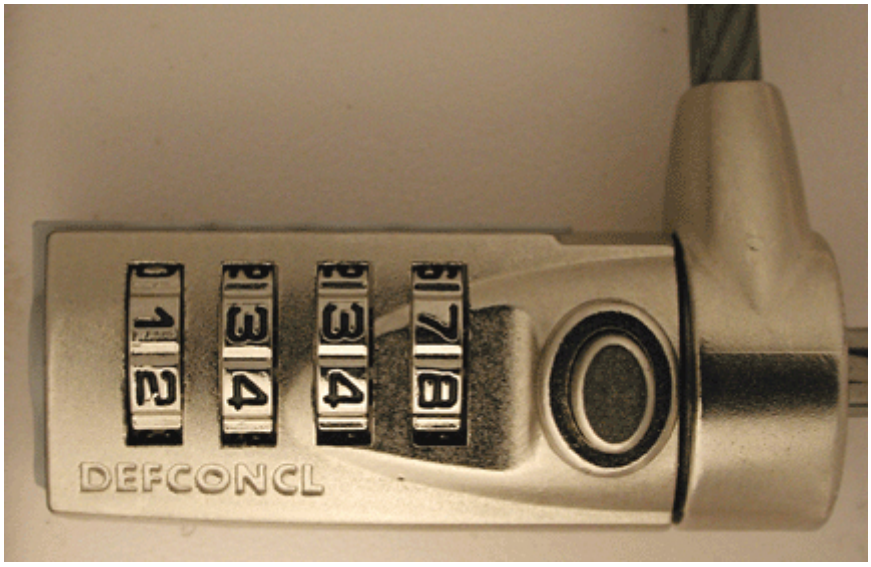
BACKGROUND

In August, 2004 Security.org released a Security Alert warning consumers that if they utilized the Targus DEFCON CL®, their notebook computers were at risk of theft. Since the release of that Alert, Targus has introduced two new models of the DEFCON that it represents are secure. We will review the earlier method of compromising the original DEFCON product, and then analyze their new design and its security vulnerabilities. This release coincides with a companion article that can be found on www.engadget.com.

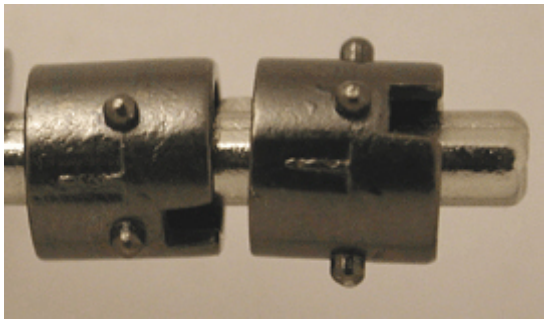
COVERT METHOD OF ENTRY

2004 Defcon CL Bypass

In the 2004 alert, a trivial decoding procedure was disclosed which could be accomplished in seconds, with no damage to the lock and which required little or no skill. The technique for the original Defcon is described below.



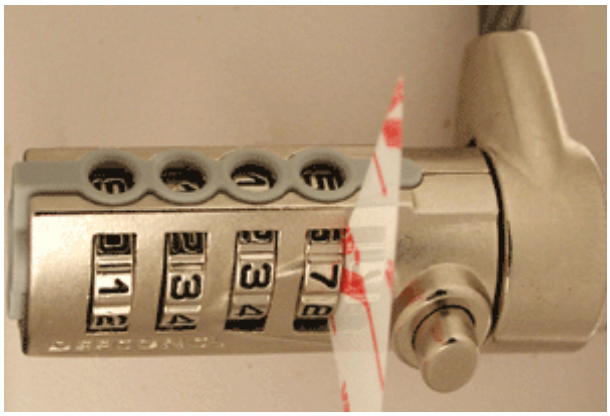
The decoding procedure is possible because of the design of this device. Four individual thumb-wheels are utilized to derive the combination. They are linked to rotating disks that each contain a gate, shown in the photograph. Each of these gates must be properly aligned to allow a fence, controlled by the push button, to move through the gates in order to retract the locking mechanism that engages with the laptop. The two disks are shown with different gate positions. Probing of each disk would provide an indication of the location and alignment of each gate, which would yield the correct combination. The position of the gate for each wheel corresponds to the number of the combination for that wheel. No correction must be made. Thus, the paper or plastic probe is run over each wheel until the gate is found, as shown in the photograph. The identified digit for each wheel is the correct number, although it does not appear in the window where the combination is read. To open the lock, simply move each thumb-wheel so that the number appears in the window.



A piece of plastic, paper, shim, or other thin material may be inserted, as shown, behind each wheel in order to feel the position of each gate. This results from the poor tolerance between the lock body and each thumb wheel. This bypass technique is a well known procedure with other similar types of combination

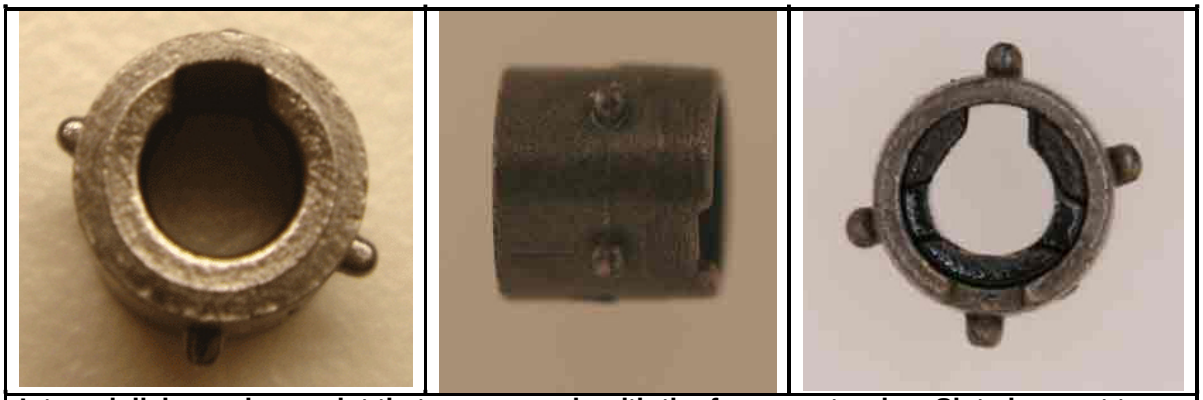
locks. Decoding of the gates takes a few seconds, resulting in the correct combination being derived. In the photograph below, a thin piece of plastic (.003") is used to feel the gate for each wheel. The corner of the plastic is run across each wheel as it is rotated. The plastic or paper will catch in the gate during rotation.

Once decoded, the lock may then be removed from the laptop, or programmed for another code, which would result in a lockout of the owner. The ability to derive the combination and reprogram the lock is clearly worrisome and constitutes a security risk.

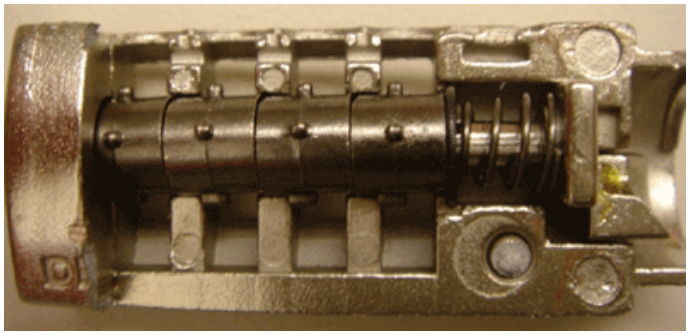


2006 Defcon CL models: PA410U and ASP10US

Targus heeded the warnings contained within our original Alert and redesigned the DEFCON ® CL to prevent the documented attack. Gate reading and decoding by probing the edge of the wheel is no longer possible because the gates have been moved from the exterior of the discs to the interior cylinders as seen in the following photographs:



Internal disk now has a slot that corresponds with the fence protrusion. Slot shown at top of disk that mates with the fence, shown below. Note in the center photograph that there is a slight gate indentation but it is masked, which make edge probing difficult.

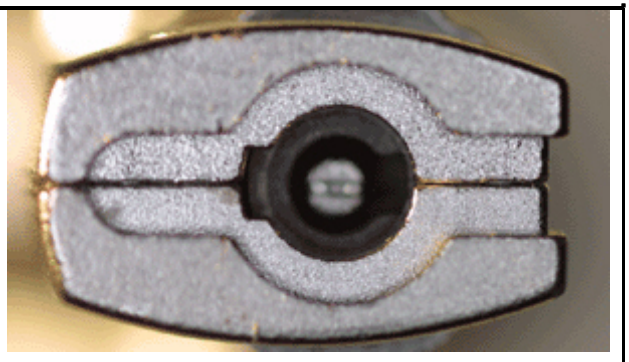


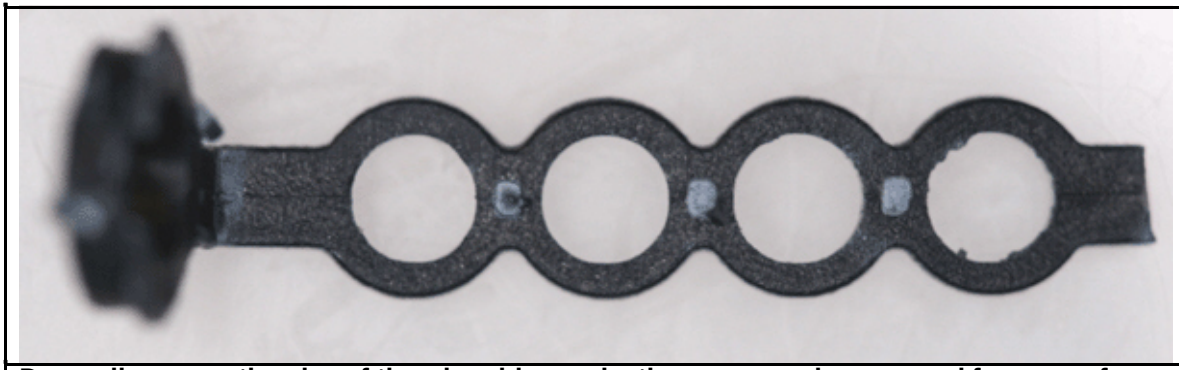


The top photograph shows four internal disks. The outer disks are indexed to the tabs that are shown protruding from the surface. When the lock is eprogrammed, the relationship between the outer and inner disk is changed, but the gate position always remains the same.

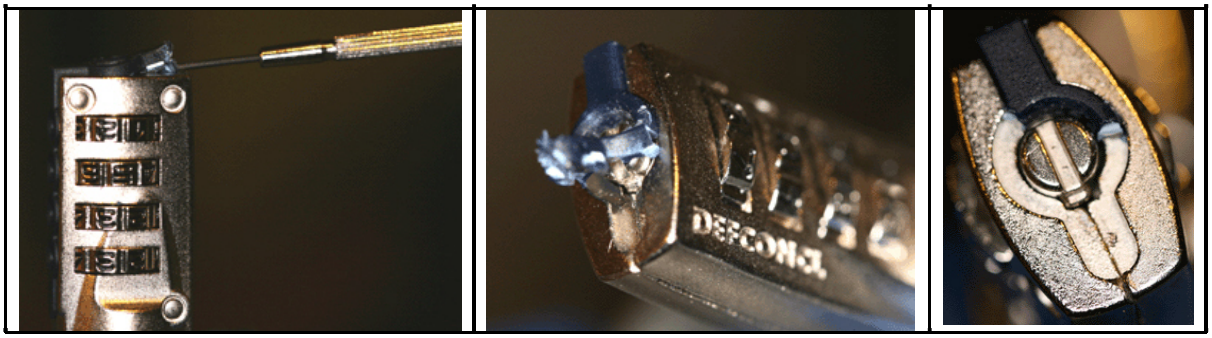
Although Targus modified their design, these gates remain exposed externally and can be easily and quickly decoded with no damage to the lock, and with little training. Decoding is accomplished via the small combination change screw on the end of the lock. The latest design requires that each of the four disks be rotated so that the elongated slot (gate) mates with the movable fence that interacts with all wheels. This fence is pushed forward by the action of the release button; each slot must be properly aligned with a protrusion of the fence in order that the lock can be opened.

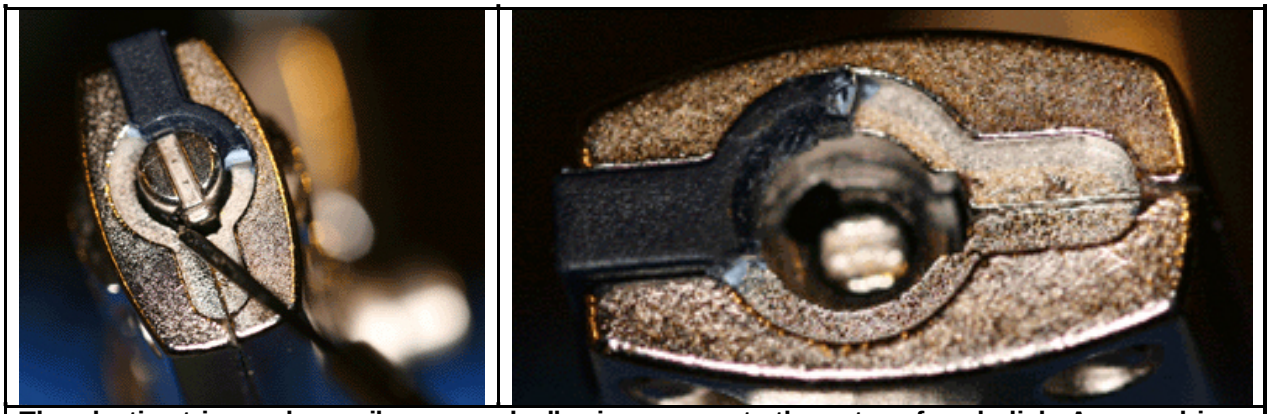






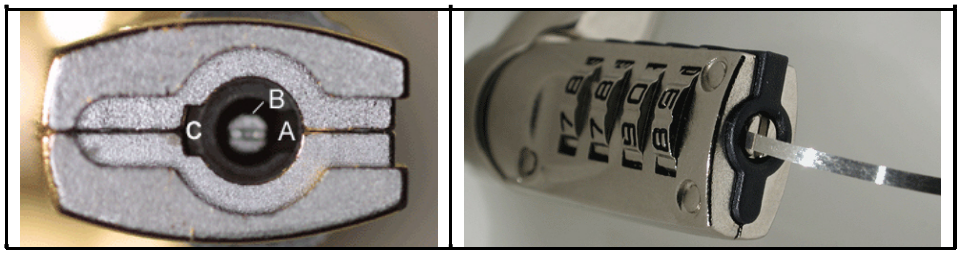
Depending upon the size of the wire shim, a plastic cover may be removed for ease of access to the internal wheels and their gates. If a shim of less than .015" is utilized, then the plastic cover may be left in place. In reality, this piece of plastic really provides the only security against decoding with a paper clip.





The plastic strip can be easily removed, allowing access to the gates of each disk. A screwdriver or BIC lighter will allow removal in seconds, thereby exposing the gates.

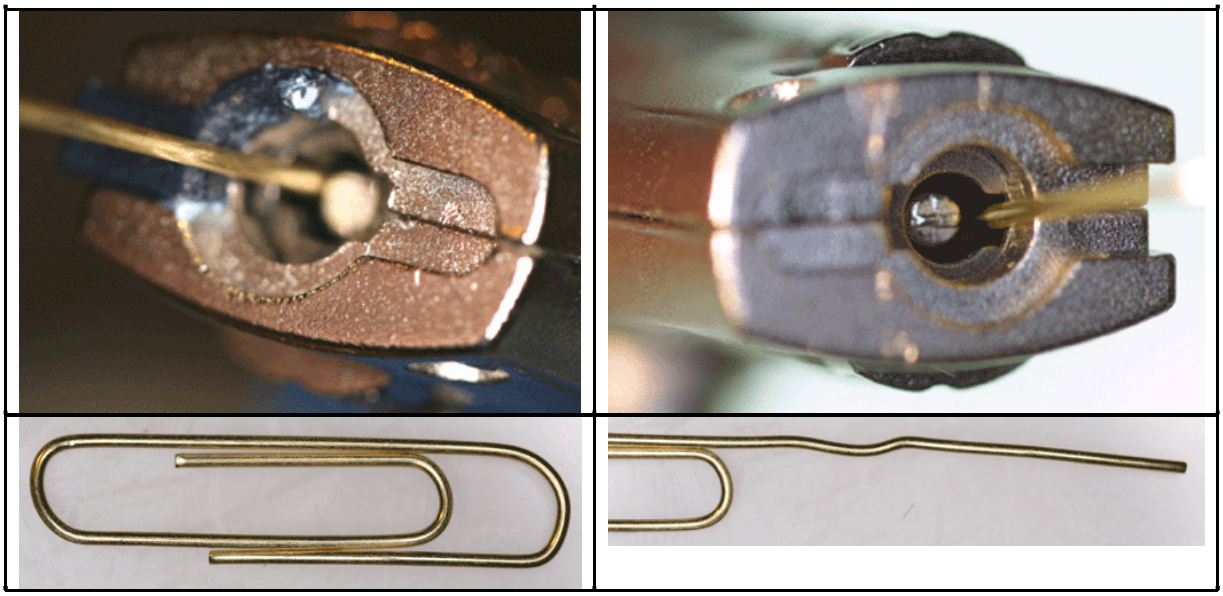
Decoding is accomplished by inserting a small wire shim in the exposed gate opening, either with or without the plastic cover removed. The wire will extend only to the first wheel, and then will be blocked, until rotated to align the gate with the position of the wire. When this occurs, the wire can be pushed forward to make contact with the second wheel. In sequence, each disk is rotated until the wire can be pushed through all the gates. When all four wheels have been rotated to the proper position, the numbers that appear at the index line must be offset by the position of the shim.



If the shim is placed at “C”, the number in the viewing window is the actual combination. If the shim is located at “A”, then the offset is 5, and if the shim is placed at “B”, then 3 must be added to the decoded number to derive the combination.



Any wire shim that is .015” or less in thickness can be utilized without the need to remove the plastic cover. A paper clip, measuring .032” can be inserted easily at position “A” and the lock can be decoded in seconds with the back of the lock exposed. The procedure to decode the position of each gate is quite straightforward and can be accomplished quickly. In the photograph above, a shim was cut from the aluminum beer can. The material thickness is .005”.



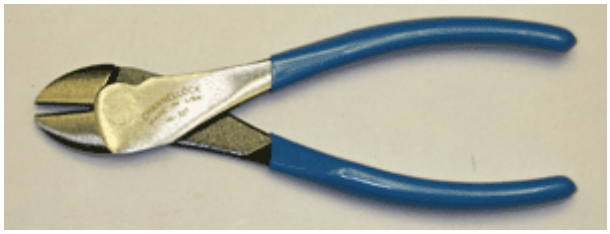
Once decoded, the lock may then be removed from the laptop, or programmed for another code, which would result in a lockout of the owner. In the opinion of the authors, Targus has learned little from their original mistake and continues to put laptop users at a significant risk of loss and theft.

FORCED METHOD OF ENTRY

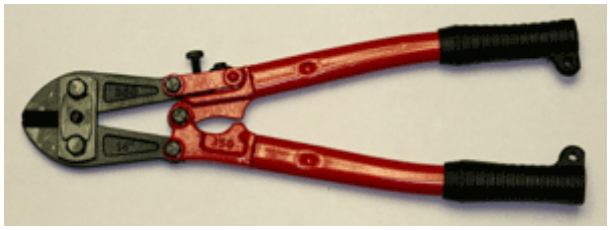
We tested the standard and armored Defcon CL cables for their resistance to cutting by commonly available diagonal cutters and bolt cutters. The cables for both locks could be severed rapidly. Although Targus advertises that their new armored Defcon is the most cut-resistant in the industry, our tests indicate otherwise. As demonstrated in the accompanying video, even the armor cable can be cut with the commonly available diagonal cutters shown below.

DEFCON CL Model P41OU Standard Cable

The standard Defcon CL utilizes a .165” diameter cable that can be easily cut with a pair of seven-inch diagonal cutters within a few seconds. From the standpoint of forced removal, this lock offers virtually no resistance and should not be relied upon for any measure of security against this form of attack.



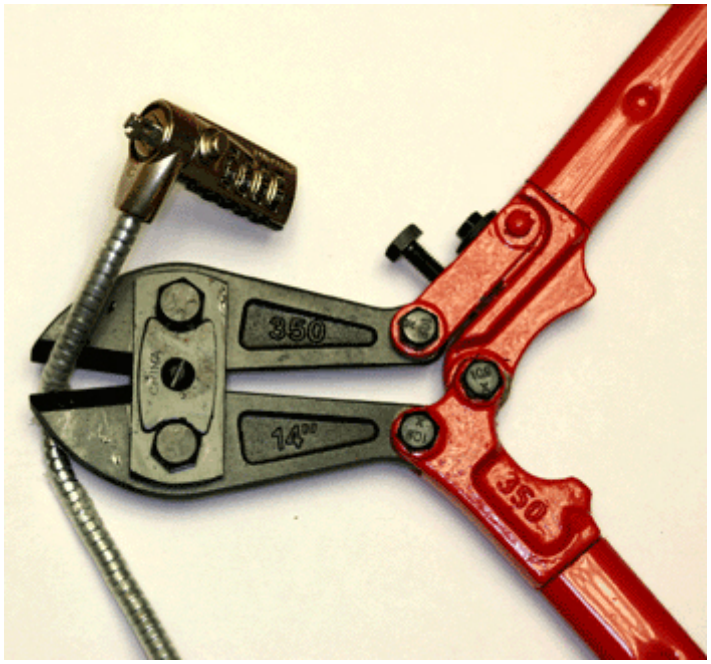
TARGUS DEFCON CL® MODEL ASP10US ARMORED CABLE



Targus has attempted to produce a tough cable that is supposed to be highly resistant to attack by cutters. The outer diameter of the cable, without plastic coating, is .245”. The PVC covering adds another .010”, for a total diameter of .265”. The inner cable is only .080” thick, or half that of the standard Defcon.

The fourteen-inch pair of cutters shown above will cut the outer and inner cable in a few seconds. However, for those who consider that these would be too large to conceal, the seven-inch diagonal cutters may also be utilized with little added difficulty to sever the internal cable, once exposed.

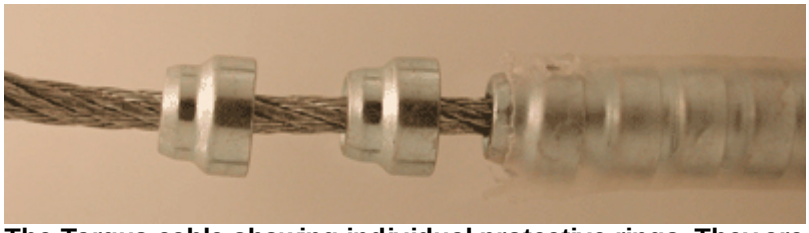
The claims by Targus as to cut resistance are misleading and only partially accurate. The cable is very resistant to cutting if you attempt to sever the cable with standard cutters with the cable in its natural state; that is, not bent. So long as the thieves abide by this rule, all will be secure! Unfortunately, this is not likely.





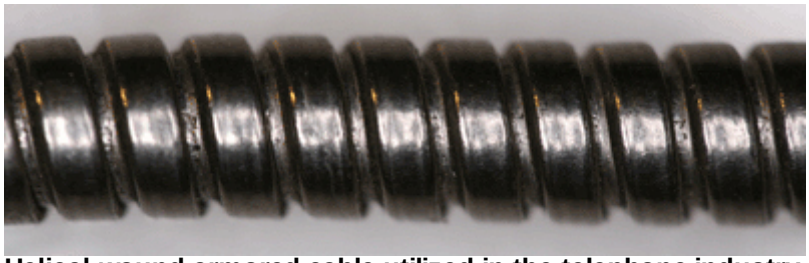
The armor cable and inner core can be easily cut with the fourteen-inch pair of bolt cutters.

Targus has chosen an armor technology that we believe is not really secure for the purpose intended. The cable consists of a series of outer steel rings that protect a reduced diameter inner cable. Unlike other forms of armor such as are employed in the telephone industry to protect payphone handsets, the Targus outer sheath fails when bending is applied. In order to produce a true armor protection, it is required that the links are interlocked to prevent the form of attack that we employed with the Targus. In the photograph below, the links are not locked together, but rather are pressed tightly against each other solely by virtue of the way the cable is assembled. Targus utilizes a .010" thick plastic covering over the entire cable length. We are not sure whether they did this for scratch resistance or for security. If the reason was to protect the outer rings, then it has little affect, and as shown, can be easily cut or melted.



The Targus cable showing individual protective rings. They are only held together by the PVC coating and total length of the cable.

The photograph above shows how the rings are linked together. When bending is applied to the cable, the inner core can be exposed and easily cut. The photograph below shows an armored cable that protects a telephone handset. Note that it is wound from a continuous piece of metal ribbon and is much more difficult to separate, using the Targus method of attack.



Helical-wound armored cable utilized in the telephone industry
Interlocks each segment to provide more resistance against the method

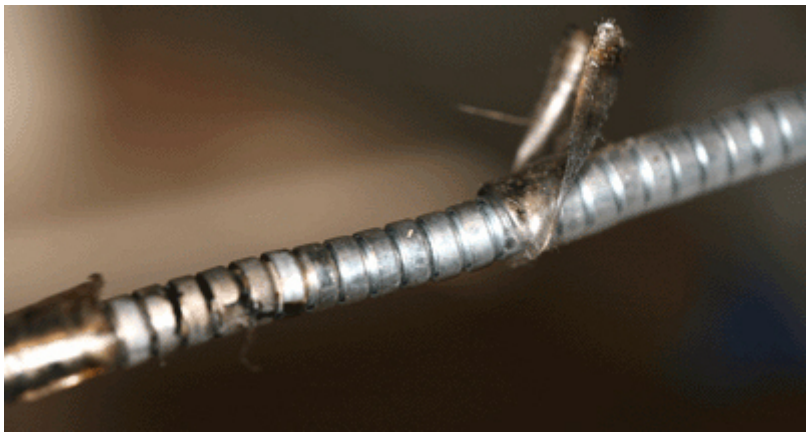
of attack to compromise the Targus Defcon.

In order to cut the Targus armored cable, it must be bent at an acute angle in order to expose the inner core. The plastic coating must be broken, then, the seven-inch diagonal cutters can easily cut the cable, as shown. The PVC outer layer can be removed with a razor blade, knife, exacto-knife, or can be melted.





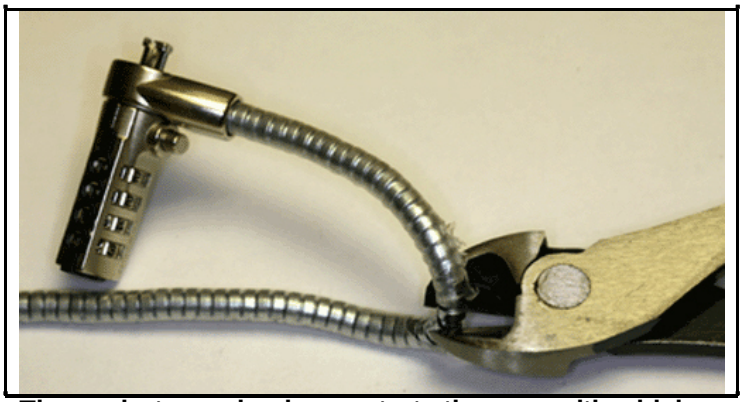




The plastic covering must be removed by either cutting or burning. Note that once the PVC begins to burn, it will continue on its own. This was ignited with a pocket BIC lighter.







These photographs demonstrate the ease with which the armor cable can be cut, once the outer covering is bent to expose the inner core.



This armored cable is utilized in the telephone industry to protect handsets. Note that even with extreme bending, the inner core is not exposed.

CONCLUSIONS

Although the Defcon CL armored cable appears to be virtually invincible, it is not. It can be quickly compromised with readily available tools that can be easily concealed. Security for this product relies upon the armored cable and the lock. Each can be bypassed quickly. The cable can be cut with a standard pair of wire cutters and a pliers to bend the cable in order to expose the inner core. The lock can be decoded through the use of a thin piece of wire or paper clip.

We do not believe that this lock is secure against either covert or forced means of entry and should be evaluated by the individual user to determine its suitability, based upon security requirements. Targus might consider employing engineers that actually understand the most basic methods of defeat. If in fact they do

possess such competence, then they are oblivious to the security needs of the consumers that rely upon them to secure their laptops. But then, Targus does not guarantee the security of these products, just their workmanship to be free from defects.

® DEFCON CL is a registered trademark of Targus.